Ghassan Haouem

Traccia:
Sulla base dell'esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Requisito:
Seguire gli step visti in lezione teorica. Prima, configurate l'ip della vostra Kali con 192.168.1.25 e l'ip della vostra Metasploitable con 192.168.1.40

Scansione completa delle porte con Nmap

Per ampliare la nostra visione sui servizi esposti su *Metasploitable*, abbiamo eseguito una scansione con *Nmap*, specificando le opzioni `-sV -T5` per identificare la versione dei servizi e velocizzare la scansione. Il comando usato è stato:

```
nmap -sV -T5 192.168.1.40
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -T5 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-12 07:55 EST
Nmap scan report for 192.168.1.40
Host is up (0.000073s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:C5:3B:59 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:li

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.47 seconds
```

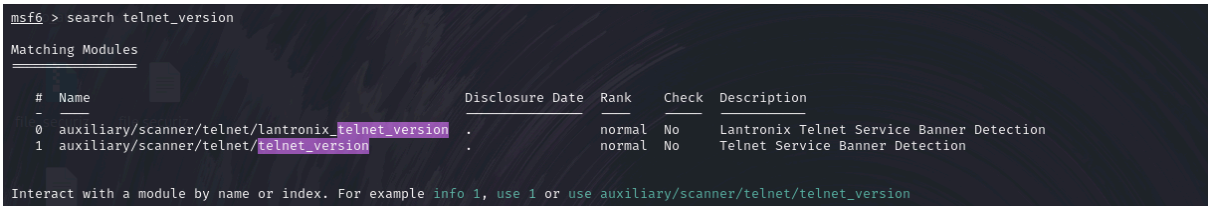
I risultati della scansione hanno mostrato numerosi servizi in esecuzione e porte aperte, tra cui il **Telnet** su porta 23.

Questa scansione ci ha fornito una panoramica dei servizi attivi, alcuni dei quali (come *vsftpd*, *Samba* e *Telnet*) sono noti per avere vulnerabilità specifiche.

Ricerca del modulo di scansione Telnet in Metasploit

Dopo aver avviato Metasploit con il comando `msfconsole` abbiamo avviato *Metasploit* e cercato un modulo specifico per rilevare la versione del servizio *Telnet* in esecuzione su *Metasploitable*. Utilizzando il comando:

```
search telnet_version
```



Abbiamo identificato due moduli:

- `auxiliary/scanner/telnet/lantronix_telnet_version`
- `auxiliary/scanner/telnet/telnet_version`

Abbiamo scelto di utilizzare il modulo `auxiliary/scanner/telnet/telnet_version` , che permette di effettuare una semplice scansione di *banner* per identificare il servizio *Telnet*.

Configurazione ed esecuzione del modulo Telnet Version

Una volta selezionato il modulo `telnet_version`, lo abbiamo configurato impostando l'indirizzo IP di *Metasploitable* come *target* (192.168.1.40) tramite il comando:

```
set RHOSTS 192.168.1.40
```

Successivamente, abbiamo eseguito il modulo con il comando `exploit` , che ha attivato una scansione del servizio *Telnet* sulla porta 23 (la porta di default per Telnet). Il risultato ha mostrato informazioni sul servizio attivo su *Metasploitable*, compreso un *banner* con l'avviso di non esporre la VM a reti non sicure. Queste informazioni ci confermano che il servizio *Telnet* è attivo e potenzialmente vulnerabile.